UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,591	11/27/2001	Gal Almogy	1104-US	9853

24505 7590 05/04/2005

DANIEL J SWIRSKY
PO BOX 2345
BEIT SHEMESH, 99544
ISRAEL

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/993,591	ALMOGY ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-138* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-138* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/22/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-138 are presented for examination.

2. The abstract of the disclosure is objected to because it is too short. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 20-22, 61-62, 74, 92, and 127 are rejected under 35 U.S.C. 102(e) as being anticipated by Kirsch et al. (Kirsch, Patent No.: US 6,772,196 B1).

As per claims 1 and 74, Kirsch teaches a computer virus detection and containment system/method comprising:

at least one computer configured with at least one decoy address (Kirsch col. 5 lines 31-34, and lines 42-44); and

a server (Kirsch Fig. 1 No. 16; UEM signature server) operative to:

identify activity occurring at said computer (Kirsch col. 4 lines 65-66), said activity involving said decoy address (Kirsch col. 6 lines 1-8).

As per claims 20, 61, and 127, Kirsch teaches a system/method wherein at least one characteristic of said decoy message sent to said computer is known in advance to said computer (Kirsch col. 6 lines 27-38, and fig. 1 No. 18).

As per claims 21 and 62, Kirsch teaches a system/method wherein at least one characteristic of said decoy message is known in advance to said server (Kirsch col. 6 lines 27-38, and fig. 1 No. 18).

As per claims 22 and 92, Kirsch teaches a system/method wherein said computer is operative to send a plurality of decoy messages to a plurality of decoy addresses at various frequencies (Kirsch col. 5 lines 14-33).

5. Claims 27-29, 31-33, 37-39, 42-51, 67-73, 96-101, 105-107, 110-118, and 132-138 are rejected under 35 U.S.C. 102(e) as being anticipated by Tarbotton et al. (Tarbotton, Patent No. US 6,757,830 B1).

As per claims 27 and 96, Tarbotton teaches a computer virus detection and containment system/method comprising:

a plurality of computers (Tarbotton No. 2 and 4); and

a server (Tarbotton No. 8, 10, and 12) operative to:

collect information regarding target behavior detected at any of said computers (Tarbotton col. 2 lines 1-3 and fig. 3 No. 30);

correlate said target behavior (Tarbotton col. 6 lines 42-55, and fig. 3 No. 28);

determine whether said correlated target behavior information corresponds to a predefined suspicious behavior pattern (Tarbotton col. 5 lines 65-67, and fig. 2 No. 20), and, if so;

perform at least one virus containment action (Tarbotton col. 6 lines 47-55, and fig. 3 No. 28).

As per claims 28 and 97, Tarbotton teaches a system/method wherein any of said computers is configured with at least one target behavior profile, and wherein said configured computer is operative to detect said target behavior and report the presence of said target behavior to said server (Tarbotton col. 5 lines 31-41).

As per claims 29 and 98, Kirsch teaches a system/method wherein said server is configured with at least one target behavior profile, and wherein said server is operative to detect said target behavior at any of said computers (Tarbotton col. 5 lines 31-41).

As per claims 31, and 99, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Tarbotton teaches a system/method wherein said virus containment action is preventing any of said messages sent by said computer from being forwarded to their intended recipients (Tarbotton col. 6 lines 49-52).

As per claims 32 and 100, Tarbotton teaches a system/method wherein said virus containment action is notifying a user at any of said computers that said suspicious behavior pattern has been detected (Tarbotton col. 6 lines 53-55).

As per claims 33 and 101, Tarbotton teaches a system/method wherein said virus containment action is notifying a system administrator that said suspicious behavior pattern has been detected (Tarbotton col. 6 lines 53-55).

As per claims 37 and 105 Tarbotton teaches a computer virus detection and containment system/method comprising:

a computer operative to send messages (Tarbotton col. 5 lines 34-37); and

a server operative to:

receive messages sent from said computer (Tarbotton col. 2 lines 1-3),

buffer any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients (Tarbotton col. 5 lines 59-67, and col. 6 lines 56-61); and

perform at least one virus containment action upon said buffer (Tarbotton col. 6 lines 47-55, and fig. 3 No. 28).

As per claims 38, and 106, Tarbotton teaches a system/method wherein said virus containment action is preventing any of said messages sent by said computer from being forwarded to their intended recipients (Tarbotton col. 6 lines 49-52).

As per claims 39 and 107, Tarbotton teaches a system/method wherein said virus containment action is preventing any messages from being forwarded from said buffer to their intended destinations (Tarbotton col. 6 lines 49-52).

As per claims 42 and 110, Tarbotton teaches a system/method wherein said delay period is variably adjustable according to any of a plurality of desired levels of system alertness (Tarbotton col. 2 lines 35-41 and col. 8 lines 63-col. 9 lines 2).

As per claims 43 and 111, Tarbotton teaches a system/method wherein said delay period is variably adjustable according to any of a plurality of types of messages (Tarbotton col. 2 lines 35-41 and col. 8 lines 63-col. 9 lines 2).

As per claims 44 and 112, Tarbotton teaches a system/method wherein said delay period is variably adjustable according to any of a plurality of types of attachments (Tarbotton col. 2 lines 35-41 and col. 8 lines 63-col. 9 lines 2).

As per claims 45 and 113, Tarbotton teaches a system/method wherein said delay period is variably adjustable for different users (Tarbotton col. 2 lines 35-41 and col. 8 lines 63-col. 9 lines 2).

As per claims 46 and 114, Tarbotton teaches a system/method wherein said delay period is variably adjustable for different uses activities (Tarbotton col. 2 lines 35-41 and col. 8 lines 63-col. 9 lines 2).

As per claims 47 and 115, Tarbotton teaches a system/method wherein said delay period is variably adjustable for different destinations (Tarbotton col. 2 lines 35-41 and col. 8 lines 63-col. 9 lines 2).

As per claims 48 and 116, Tarbotton teaches a system/method wherein said server is operative to:

increase said delay period by a predetermined amount of time upon detecting suspected virus activity (Tarbotton col. 3 lines 36-46), and

perform said virus containment action if, during said increased delay period, additional suspected virus activity is detected and no indication that said activity is not virus related is received (Tarbotton col. 6 lines 62-col. 7 lines 13).

As per claims 49 and 117, Tarbotton teaches a system/method wherein said server is operative to:

reduced said delay period to its previous level if, during said increased delay period, additional suspected virus activity is not detected (Tarbotton col. 3 lines 36-65).

As per claims 50 and 118, Tarbotton teaches a system/method wherein said server is operative to:

reduced said delay period to its previous level if, during said increased delay period, an indication that said activity is not virus related is received (Tarbotton col. 3 lines 36-65).

As per claim 51 Tarbotton teaches a system/method wherein said messages are electronic mail messages (Tarbotton fig. 3 No. 24).

As per claims 67 and 132, Tarbotton teaches a computer virus detection and containment system comprising:

a plurality of servers, each configured to maintain a virus detection sensitivity level (Tarbotton Fig. 1 No. 8, 10, 12, and 14); and

multiple pluralities of computers, each plurality of computers being in communication with at least one of said servers (Tarbotton Fig. 1 No. 2 and 4);

wherein each of said servers is operative to:

detect suspected virus activity at any of its related plurality of computers notify any of said servers of said detected suspected virus activity (Tarbotton col. 5 lines 31-47), and

adjust said virus detection sensitivity level according to a predefined plan (Tarbotton col. 5 lines 31-47 and fig. 3 No. 28).

As per claims 68 and 133, Tarbotton teaches a system/method wherein said predefined plan is in predefined relation to said notification (Tarbotton col. 6 lines 47-55).

As per claims 69 and 134, Tarbotton teaches a system/method wherein said adjustment is a lengthening of a message buffer delay period (Tarbotton col. 5 lines 59-67, and col. 6 lines 59-61).

As per claims 70 and 135, Tarbotton teaches a system/method wherein said adjustment is selecting virus containment actions which are performed when a suspected virus is detected at any of said computers (Tarbotton Fig. 3 No. 28).

As per claims 71 and 136, Tarbotton teaches a system/method wherein said adjustment is selecting target behavior to be tracked at said computers (Tarbotton col. 2 lines 35-41).

As per claims 72 and 137, Tarbotton teaches a system/method wherein said adjustment is selecting which correlations of target behavior are performed for target behavior detected at any of said computers (Tarbotton col. 2 lines 35-41, col. 6 lines 42-55, and fig. 3 No. 28).

As per claims 73 and 138, Tarbotton teaches a system/method wherein said adjustment is selecting quantifications of suspicious behavior patterns (Tarbotton col. 5 lines 65-67, and fig. 2 No. 20).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2-9, 13-18, 23-26, 30, 40-41, 52-57, 63-66, 75-81, 85-88, 90-91, 93-95, 108-109, 119-123, and 128-131 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kirsch et al. (Kirsch, Patent No.: US 6,772,196 B1) in view of Tarbotton et al. (Tarbotton, Patent No. US 6,757,830 B1).

As per claims 17 and 88, Kirsch teaches a system/method comprising:

a computer configured with at least one decoy address and operative to periodically address a decoy message to one or more of said decoy addresses (Kirsch col. 5 lines 31-34, lines 42-44, and lines 56-58); and

a server operative to:

receive messages sent from said computer (Kirsch col. 5 lines 56-58),

determine whether any of said messages are addressed to any of said decoy addresses (Kirsch col. 5 lines 14-33, and col. 6 lines 27-38), and

upon determining that at least one of said messages is addressed to any of said decoy addresses, determine whether said decoy-addressed message is a valid decoy message (Kirsch col. 5 lines 14-33, and col. 7 lines 4-7), and

Kirsch does not teach performing at least one virus containment action.

However Tarbotton teaches a computer virus detection and containment method/system and perform at least one virus containment action when virus is detected by comparing the received email with the virus definition stored on server (Tarbotton col. 5 lines 59-col. 6 lines 3 and fig. 2 No. 28).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Tarbotton within the system of Kirsch because it would allow to identify the infected email and disinfect the infected email by comparing the received email with the known/predetermined virus definition (Tarbotton col. 6 lines 42-55).

As per claims 52 and 119, Kirsch teaches a computer virus detection and containment system comprising:

at least one computer configured with at least one decoy address (Kirsch col. 5 lines 31-34, lines 42-44, and lines 56-58); and

a server configured with said decoy address (Kirsch col. 5 lines 14-33, and lines 56-58) and operative to periodically send to said computer at least one decoy message addressed from said decoy address (Kirsch col. 5 lines 56-58);

wherein said computer is operative to:

receive messages sent from said server (Kirsch col. 3 lines 29-34, and col. 5 lines 56-58),

determine whether any of said messages sent from said server are addressed from said decoy address (Kirsch col. 3 lines 29-34, and col. 5 lines 14-33, and col. 6 lines 27-38), and

upon determining that at least one of said messages sent from said server is addressed from said decoy address, send a response decoy message addressed to said decoy address to said server in response to receiving said decoy message from said server (Kirsch col. 3 lines 29-34, and col. 5 lines 14-33, and col. 7 lines 4-7), and

wherein said server is operative to:

receive messages sent from said computer (Kirsch col. 5 lines 56-58),

determine whether any of said messages sent from said computer are addressed to said decoy address (Kirsch col. 5 lines 14-33, and col. 6 lines 27-38), and

upon determining that at least one of said messages sent from said computer is addressed to said decoy address, determine whether said decoy-addressed message is a valid decoy message (Kirsch col. 5 lines 14-33, and col. 7 lines 4-7), and

Kirsch does not teach performing at least one virus containment action.

However Tarbotton teaches a computer virus detection and containment method/system and perform at least one virus containment action when virus is detected by comparing the received email with the virus definition stored on server (Tarbotton col. 5 lines 59-col. 6 lines 3 and fig. 2 No. 28).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Tarbotton within the system of Kirsch because it would allow to identify the infected email and disinfect the infected email by comparing the received email with the known/predetermined virus definition (Tarbotton col. 6 lines 42-55).

As per claims 2 and 75, Kirsch teaches all the subject matter as described above. Kirsch does not teach performing at least one virus containment action upon identifying said activity.
However Tarbotton discloses a computer virus detection and containment method/system and perform at least one virus containment action when virus is detected by comparing the received email with the virus definition stored on server (Tarbotton col. 5 lines 59-col. 6 lines 3 and fig. 2 No. 28).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Tarbotton within the system of Kirsch

because it would allow to identify the infected email and disinfect the infected email by comparing the received email with the known/predetermined virus definition (Tarbotton col. 6 lines 42-55).

As per claims 3 and 76, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Kirsch teaches a system/method wherein:

said server is operative to:

receive messages sent from said computer (Kirsch col. 5 lines 56-58),

determine whether any of said messages are addressed to any of said decoy addresses (Kirsch col. 5 lines 14-33, and col. 6 lines 27-38), and

upon determining that at least one of said messages is addressed to any of said decoy addresses (Kirsch col. 5 lines 14-33, and col. 7 lines 4-7),

Tarbotton teaches a computer virus detection and containment method/system and performing a virus containment action when virus is detected by comparing the received email with the virus definition stored on server (Tarbotton col. 5 lines 59-col. 6 lines 3 and fig. 2 No. 28). The rational for combining are the same as claim 2 above.

As per claims 4, 18, 30, and 56, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Kirsch teaches a system/method wherein said computer is configured to operate as said server (Kirsch col. 3 lines 29-34).

As per claims 16, 26, and 66, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Kirsch teaches a system/method wherein said messages are electronic mail messages (Kirsch col. 2 lines 64-66).

As per claims 5, and 77, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Tarbotton teaches a system/method wherein said virus containment action is preventing any of said messages sent by said computer from being forwarded to their intended recipients (Tarbotton col. 6 lines 49-52). The rational for combining are the same as claim 2 above.

As per claims 6 and 78, Kirsch and Tarbotton teach all the subject matter as described above. In addition, a system/method wherein said virus containment action is forwarding any of said messages that are addressed to a decoy address to a third party for analysis (Tarbotton col. 5 lines 31-41, and Kirsch col. 5 lines 56-58). The rational for combining are the same as claim 2 above.

As per claims 7 and 79, Kirsch and Tarbotton teach all the subject matter as described above. In addition, a system/method wherein said virus containment action is notifying a user at said computer that at least one of said messages is addressed to any of said decoy addresses (Tarbotton col. 6 lines 53-55 and Kirsch col. 5 lines 14-33). The rational for combining are the same as claim 2 above.

As per claims 8 and 80, Kirsch and Tarbotton teach all the subject matter as described above. In addition, a system/method wherein said virus containment action is notifying a system

administrator that at least one of said messages is addressed to any of said decoy addresses (Tarbotton col. 6 lines 53-55 and Kirsch col. 5 lines 14-33). The rational for combining are the same as claim 2 above.

As per claims 9, 57, 81, and 123, Kirsch and Tarbotton teach all the subject matter as described above. In addition, a system/method wherein said virus containment action is preventing any messages at said server from being forwarded to their intended destinations (Tarbotton col. 6 lines 49-52 and Kirsch col. 5 lines 14-33). The rational for combining are the same as claim 2 above.

As per claims 13, 23, 63, 93, 85, and 129 Kirsch and Tarbotton teach all the subject matter as described above. In addition, Tarbotton teaches a system/method wherein said server is operative to buffer any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients (Tarbotton col. 5 lines 59-67). The rational for combining are the same as claim 2 above.

As per claims 14, 24, 40, 86, 94, and 108, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Tarbotton teaches a system/method wherein said virus containment action is changing said delay period for all of said messages sent by said computer and buffered by said server (Tarbotton col. 5 lines 59-67, and col. 6 lines 56-61). The rational for combining are the same as claim 2 above.

As per claims 15, 25, 41, 87, 95, and 109 Kirsch and Tarbotton teach all the subject matter as described above. In addition, Tarbotton teaches a system/method wherein said virus containment action is changing said delay period for all messages buffered by said server (Tarbotton col. 5 lines 59-67, and col. 6 lines 56-61). The rational for combining are the same as claim 2 above.

As per claims 53 and 120, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Kirsch teaches a system/method wherein said response decoy message is the same as said decoy message received from said server (Kirsch col. 3 lines 29-34, and col. 5 lines 14-33, and col. 7 lines 4-7).

As per claims 54 and 121, Kirsch and Tarbotton teach all the subject matter as described above. In addition, a system/method wherein said computer is operative to open said decoy message received from said server prior to sending said response decoy message to said server (Kirsch col. 3 lines 29-34, & col. 5 lines 14-33, and Tarbotton col. 5 lines 59-67). The rational for combining are the same as claim 2 above.

As per claims 55 and 122, Kirsch and Tarbotton teach all the subject matter as described above. In addition, a system/method wherein said computer is operative to open an attachment attached to said decoy message received from said server prior to sending said response decoy message to said server (Kirsch col. 3 lines 29-34, & col. 5 lines 14-33, and Tarbotton col. 5 lines 59-67 and col. 9 lines 7-9). The rational for combining are the same as claim 2 above.

As per claims 64 and 130, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Tarbotton teaches a system/method wherein said virus containment action is changing said delay period for all of said messages sent by said computer and buffered by said server (Tarbotton col. 8 lines 15-56 and fig. 5). The rational for combining are the same as claim 2 above.

As per claims 65 and 131, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Tarbotton teaches a system/method wherein said virus containment action is changing said delay period for all messages buffered by said server (Tarbotton col. 8 lines 15-56 and fig. 5). The rational for combining are the same as claim 2 above.

As per claim 90, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Tarbotton teaches a system/method and further comprising configuring a server at which said messages are received with a schedule, and wherein said periodically sending step comprises sending said decoy messages according to said schedule (Kirsch col. 5 lines 56-58). The rational for combining are the same as claim 2 above.

As per claim 91, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Kirsch teaches a method and further comprising configuring a server at which said messages are received with at least one characteristic of said decoy message (Kirsch col. 5 lines 14-33, lines 43-45, and 56-58).

As per claim 128, Kirsch and Tarbotton teach all the subject matter as described above. In addition, Kirsch teaches a method wherein said configuring step comprises configuring said computer with at least one characteristic of said decoy message (Kirsch col. 5 lines 14-33, lines 43-45, and 56-58).

8. Claims 10-12, 19, 34-36, 58-60, 82-84, 89, 102-104, and 124-126 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kirsch et al. (Kirsch, Patent No.: US 6,772,196 B1) in view of Tarbotton et al. (Tarbotton, Patent No. US 6,757,830 B1), and further in view of Chefalas et al. (Chefalas, Pub. No. US 2002/0116639 A1).

As per claims 10, 34, 58, 82, 102, and 124, Kirsch and Tarbotton teach all the subject matter as described above. Kirsch and Tarbotton does not explicitly teach wherein said virus containment action is revoking any privileges that said computer has to access a network.

However Chefalas teaches wherein said virus containment action is revoking any privileges that said computer has to access a network (Chefalas Fig. 6 No. 606, and fig. 7 No. 706, and page 5 par. 0051 and par. 0054).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Chefalas within the combination system of Kirsch and Tarbotton because it would prevent further spreading of the virus (Chefalas page 5 par. 0054 line 11).

As per claims 11, 35, 59, 83, 103 and 125, Kirsch, Tarbotton, and Chefalas teach all the subject matter as described above. In addition, Chefalas teaches a system/method wherein said virus containment action is revoking any privileges that said computer has to access shared network files or directories (Chefalas Fig. 6 No. 606, and fig. 7 No. 706, and page 5 par. 0051 and par. 0054). The rational for combing are the same as claim 10 above.

As per claims 12, 19, 36, 60, 84, 89, 104, and 126, Kirsch, Tarbotton, and Chefalas teach all the subject matter as described above. In addition, Chefalas teaches a system/method wherein said virus containment action is sending a command to a network device connected a network to block attempts by said computer to access said network (Chefalas Fig. 6 No. 606, and fig. 7 No. 706, and page 5 par. 0051 and par. 0054). The rational for combing are the same as claim 10 above.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Elemi Shiferaw
Art Unit 2136
April 21, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100